UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/033,700	12/27/2001	Andre Srinivasan	020581-000600US	8597

31824 7590 01/12/2005

MCDERMOTT WILL & EMERY LLP
18191 VON KARMAN AVE.
IRVINE, CA 92612-7107

EXAMINER	
WORJLOH, JALATEE	
ART UNIT	**PAPER NUMBER**
3621	

DATE MAILED: 01/12/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 10/033,700	**Applicant(s)** SRINIVASAN, ANDRE	
	Examiner Jalatee Worjloh	**Art Unit** 3621	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 27 December 2001.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-19 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-19 is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. Claims 1-19 have been examined.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claim 11 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Notice, claim 11 states "if the second certificate is trusted.....thereby verifying the first certificate; and if the first certificate is verified…", but does not provides steps if the second certificate is **not** trusted. Please revise this claim for clarity.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 18 and 19 rejected under 35 U.S.C. 102(e) as being anticipated by US Publication No. 2004/0177281 to Balaz et al.

Balaz et al. teach a datastore (i.e. "certificate authority") containing at least one certificate, wherein each of the at least one certificate is associated with a different one of at least one certificate reference, and a server (i.e. "registration authority"), wherein the server is configured to receive a certificate, to compute a certificate reference for the received certificate from data included in the certificate, (see paragraph [0086]), and wherein the server is further configured to respond to a request for a certificate, the request including a received certificate reference, by identifying and providing the one of the at least one stored certificate associated with the received certificate reference (see paragraph [0084]). As for the server configured to store the received certificate in association with the computed certificate reference in the data store, this is an intend use limitation. Therefore, "the recitation of a new intended use for an old product does not make a claim to that old product patentable" In re Schreiber, 44 USPQ2d 1429 (Fed. Cir. 1997).

Referring to claim 19, Balaz et al. disclose a public key infrastructure (virtual private network with a router, registration authority and certificate authority) configured to associate with each of the plurality of certificates a different one of a plurality of certificate references, and in response to a request including one of the plurality of certificate references, to return the corresponding one of the plurality of certificates (see paragraph [0086]), a sender (i.e. router) configured to digitally sign a message using a first private key and to send a message including the digitally signed message and a first certificate reference (see paragraph [0084]), and a recipient (i.e. registration authority) configured to receive the message, to send a request including the first certificate reference to the public key infrastructure, to receive a corresponding first certificate from the public key infrastructure, and to use the first certificate to authenticate the digitally signed message (see paragraph [0086] & [0046]). As for the public key infrastructure configured to store a plurality of certificates, this is an inherent step. It is known in the art that public key infrastructures are configured to store certificates.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 1-3,5,6 and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Publication No. 2004/0177281 to Balaz et al. in view of US Publication No. 2004/0215959 to Cook et al.

Balaz et al. disclose digitally signing a message (i.e. "request") using a first private key associated with the sender (i.e. "router"), see paragraph [0084], retrieving a first certificate reference (i.e. "serial number') associated with a first certificate, the first certificate including a first public key corresponding to the first private key and transmitting to the recipient via the network an authenticated message comprising the digitally signed message and the first certificate reference (see paragraphs [0046], [0085] & [0086]). Balaz et al. disclose a public key infrastructure that comprises a certificate authority that issues the first certificate and the associated first certificate reference (see paragraph [0086]). Balaz et al. do not expressly disclose storing the first certificate and the associated first certificate reference in a public key infrastructure. Cook et al. disclose the first certificate and the associated first certificate reference are stored in a public key infrastructure (see paragraph [0007] and [0018]). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to modify the method disclose by Balaz et al. to store the first certificate and its reference in a public key infrastructure. One of ordinary skill in the art would have been motivated to do this because it provides a secure system.

Referring to claim 2, Balaz et al. disclose transmitting the first certificate via the network to the public key infrastructure prior to transmitting the authenticated message (see paragraph [0036]).

Referring to claim 3, Balaz et al. disclose the first certificate reference is determined from an identity of the sender and a serial number of the first certificate (see paragraph [0085]).

Referring to claim 5, Balaz et al. disclose the network is the Internet (see paragraph [0032]).

Referring to claim 6, Balaz et al. disclose encrypting the message suing a second public key, wherein the recipient holds a second private key corresponding to the second public key (see paragraph [0046]).

Referring to claim 17, Balaz et al. disclose at the sender side: Balaz et al. disclose digitally signing a message (i.e. "request") using a first private key associated with the sender (i.e. "router"), see paragraph [0084], retrieving a first certificate reference (i.e. "serial number') associated with a first certificate, the first certificate including a first public key corresponding to the first private key and transmitting to the recipient via the network an authenticated message comprising the digitally signed message and the first certificate reference (see paragraphs [0046], [0085] & [0086]). Balaz et al. disclose a public key infrastructure that comprises a certificate authority that issues the first certificate and the associated first certificate reference (see paragraph [0086]) and at the recipient side: receiving the message, transmitting the first certificate reference to a public key infrastructure via the network, receiving from the public key infrastructure via the network (see paragraph [0086]) and authenticating the digitally signed message using the first public key (see paragraph [0046]). Balaz et al. do not expressly disclose storing the first certificate and the associated first certificate reference in a public key infrastructure. Cook et al. disclose the first certificate and the associated first certificate reference are stored in a public key infrastructure (see paragraph [0007] and [0018]). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to modify the method disclose by Balaz et al. to store the first certificate and its reference in a public key infrastructure. One of ordinary skill in the art would have been motivated to do this because it provides a secure system.

8. Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over Balaz et al. and Cook et al. as applied to claim 1 above, and further in view of US Publication No. 2002/0073310 to Benantar.

Balaz et al. disclose retrieving a certificate reference to a certificate, wherein the certificate s issued to an issuer of the first certificate, wherein the certificate and the associated certificate reference are stored in the public key infrastructure and transmitting a certificate reference as a portion of the authenticated message (see claim 1 above). Balaz et al. do not expressly disclose a second certificate reference associated with a second certificate. Benantar discloses a second certificate reference associated with a second certificate (see claim 1, lines 4-7). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to modify the method disclose by Balaz et al. to include a second certificate. One of ordinary skill in the art would have been motivated to do this because it provides additional security.

9. Claims 7, 9 and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Balaz et al. in view of US Patent No. 6012039 to Hoffman et al.

Balaz et al. disclose transmitting the first certificate reference to a public key infrastructure via the network, receiving from the public key infrastructure via the network a first certificate corresponding to the first certificate reference, the first certificate including a first public key (see paragraph [0086]) and if the first certificate is trusted, authenticating the digitally signed message using the first public key (see paragraph [0046]). Balaz et al. do not expressly disclose determining whether the first certificate is trusted. Hoffman et al. disclose determining whether the first certificate is trusted (see abstract, lines 20-25). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to modify the method disclose by Balaz et al. to include the step of determining whether the first certificate is trusted. One of ordinary skill in the art would have been motivated to do this because it provides security.

Referring to claim 9, Balaz et al. disclose a first certificate (see claim 7 above). Balaz et al. do not expressly disclose identifying a first issuer of the first certificate, comparing the first issuer to each of at least one trusted issuer, and if the first issuer is the same as one of the least one trusted issuer determining that the first certificate is trusted. Hoffman et al. disclose identifying a first issuer of the first certificate, comparing the first issuer to each of at least one trusted issuer, and if the first issuer is the same as one of the least one trusted issuer determining that the first certificate is trusted (see abstract, liens 20-25, col. 13, lines 5-15 and col. 10, lines 34-38). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to modify the method disclose by Balaz et al. to include the steps of disclose identifying a first issuer of the first certificate, comparing the first issuer to each of at least one trusted issuer, and if the first issuer is the same as one of the least one trusted issuer determining that the first certificate is trusted. One of ordinary skill in the art would have been motivated to do this because it prevents fraud and prohibits unauthorized individuals from communicating with the entities in the system.

Referring to claim 12, Balaz et al. disclose the network is the Internet (see paragraph [0032]).

10. Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over Balaz et al. and Hoffman et al. as applied to claim 7 above, and further in view of Cook et al.

Balaz et al. disclose a public key infrastructure that comprises a certificate authority that issues the first certificate and the associated first certificate reference (see paragraph [0086]). Balaz et al. do not expressly disclose storing in a local keystore the first certificate and the first public key. Cook et al. disclose storing in a local keystore the first certificate and the first public key (see paragraph [0007] and [0018]). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to modify the method disclose by Balaz et al. to store the first certificate and public key in a local keystore. One of ordinary skill in the art would have been motivated to do this because it provides a secure system

11. Claims 10 and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Balaz et al. and Hoffman et al. as applied to claim 7 above, and further in view of Benantar.

Balaz et al. disclose transmitting a certificate reference to a public key infrastructure via the network, receiving from the public key infrastructure a certificate corresponding to the certificate reference, the certificate including a public key associated with an issuer of the certificate (see paragraph [0086]). Balaz et al. do not expressly disclose a second certificate reference associated with a second certificate or a second public key. Benantar discloses a second certificate reference associated with a second certificate and a second public key (see claim 1, lines 4-7). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to modify the method disclose by Balaz et al. to include a second certificate reference associated with a second certificate and a second public key. One of ordinary skill in the art would have been motivated to do this because it provides additional security.

As for claim 11, see claim 7 above rejection above, in which the determination process is taught.

12. Claims 13-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Balaz et al. in view of Benantar.

Balaz et al. disclose determining whether the first certificate reference is stored within a local keystore (*notice, the certificate authority accesses its records to identify the certificate corresponding to the given serial number),* if the first certificate reference is stored within the local keystore: retrieving from the local keystore a first public key associated with the first certificate reference (*the certificate is retrieved which includes the public key and reference*), see paragraph [0086] and if the first certificate reference is not stored within the local keystore: transmitting the first certificate reference to a public key infrastructure, receiving from the public key infrastructure a first certificate, the first certificate including a first public key (see paragraph [0086]). Balaz et al. do not expressly disclose determining whether the first certificate is trusted and adding information to the local keystore, the information including at least the first certificate reference and the first public key. Benantar discloses determining whether the first certificate is trusted and adding information to the local keystore, the information including at least the first certificate reference and the first public key (see claims 1 & 7). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to modify the method disclose by Balaz et al. to include the step of determining whether the first certificate is trusted and adding information to the local keystore, the information including at least the first certificate reference and the first public key. One of ordinary skill in the art would have been motivated to do this because it provides security.

Referring to claim 14, Balaz et al. disclose authenticating the digitally signed message using the first public key (see paragraph [0046]).

Referring to claim 15, Balaz et al. disclose receiving a request form a second user (i.e. "registration authority"), the request including the unique certificate reference (*i.e. get certificate by serial number)* and transmitting the certificate to the second user in response to the request (see paragraphs [0084]-[0086]). Balaz et al. do not expressly disclose receiving a certificate from reference from data contained in the certificate and storing the certificate in association with the unique certificate reference. Benantar discloses receiving a certificate from a first user and storing the certificate in association with the unique certificate reference (see claims 1 and [0052]). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to modify the method disclose by Balaz et al. to include the steps of receiving a certificate from a first user and storing the certificate in association with the unique certificate reference ey. One of ordinary skill in the art would have been motivated to do this because it provides security.

Referring to claim 16, Balaz et al. disclose the certificate includes a subject identity and a serial number, and wherein the unique certificate reference is computed from the subject identity and the serial number (see paragraph [0085]).

Conclusion

13. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- International Publication No. WO 00/77974 to Xiao et al. discloses first and second certificates including serial numbers.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jalatee Worjloh whose telephone number is 703-305-0057. The examiner can normally be reached on Mondays-Thursdays 8:30 - 7:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James Trammell can be reached on 703-305-9768. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306 for Regular/After Final Actions and 703-746-9443 for Non-Official/Draft.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks
PO Box 1450
Alexandria, VA 22313-1450

Hand delivered responses should be brought to Crystal Park 5, 2451 Crystal Drive, Arlington, V.A., Seventh floor receptionist.

Jalatee Worjloh
Patent Examiner
Art Unit 3621

***

JAMES P. TRAMMELL
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 3600

January 6, 2005